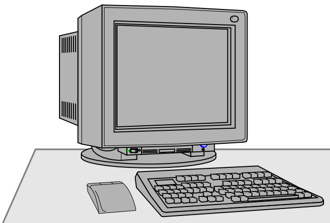
Systems Support Services - Code 5595



# Desktop

*Latest Information from the NRL Labwide ADP Program and the NRL Systems Support Team*

http://amp.nrl.navy.mil/code5595 August 11, 2000

## HRO Help Desk

The SysSupport group is now monitoring the HRO help desk requests and will eventually take over that function. This is part of a larger initiative by Code 5595 to provide, over time, a centralized labwide help desk. The concept is that a central help desk will provide a single point of contact for computer technology problems, regardless of where the problem exists.

The centralized help desk will involve a three-tiered approach to solving problems. They will assess the problem to determine if:

1. it can be handled by staff, e.g, resetting passwords
2. it needs to be farmed out to an on-site technician.
3. it needs to be referred to a subject-matter specialist, e.g., policy issue on writing RDs.

The advantage to this approach is that there should be a rapid response to any problem.

During this transition period there will likely be some glitches. However, as the help desk personnel become more familiar with the various HRO issues and applications, the scope of the first tier of help will expand. As the help desk takes on a larger proportion of the general problems, additional time will be freed up for the HRO staff to handle more specific issues. ■

## Napster Vulnerabilities

There are a number of new utilities and services on the Web that present security vulnerabilities and challenges if not configured and used properly. **Napster**, **Wrapster**, **Gnutella**, **SpinFrenzy** and **CuteMX** are several new utilities/services that present a security challenge and potential for misuse of government Information Systems (IS).

NRL Note 5239 specifically prohibits the use of NRL IS for: "*Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.*"

In addition to the issue of copyright violation, the use of Napster presents new security vulnerabilities for anybody using it on an end user host. The use of Napster on an end user host computer can essentially make that host an anonymous file server on the Internet. This sort of file or Web service without appropriate protections (wrappers, passwords, etc.) is not authorized on NRL computers. Redistribution or acquisition of copyright material such as MP3 music files is certainly not authorized.

The vulnerabilities of Napster have now increased with the introduction on the Internet of a new utility called Wrapster. Napster can be tricked into letting just about any data out of a user's desktop when combined with the new "wrapping" program called Wrapster. The Wrapster program is a well designed Trojan Horse that can make anything look like an MP3 file, which can then be remotely downloaded from a PC without the user noticing.

Anyone who has downloaded and installed the Napster client is open to exploitation. Because the code behind these programs is open source and freely available on the Web, users of both Napster and Wrapster are already creating variants of them. That means that even if vendors of intrusion-detection systems profile an appropriate attack signature, the signatures are changing, making them difficult if not impossible for intrusion detection tools to detect.

Increased vigilance and implementation of appropriate security is more important that ever. The vulnerabilities presented by Napster and other peer-to-peer applications are not just a concern at work, you should consider the risks to your personal computers at home as well. ■

**Desktop**

**Naval Research Laboratory**
**4555 Overlook Ave., S.W.**
**Washington, DC 20375-5320**

**Editor, Code 5595.2**
**Phone: (202) 767-5853**
**via e-mail:**
**syssupport@nrl.navy.mil**

**published periodically**
**distributed to: distribution list**
**d at NRL-DC**

## Catch Up on Your Training Objectives

Code 5595 is here to help you with your training needs. In addition to the instructor led classes that are offered periodically, we now offer both on-line computer-based training and multimedia (VHS tapes & Cdrom) training materials for checkout. There are older scientific training materials for checkout as well as some new up-to-date titles to help you get your Microsoft Certifications or learn how to create a web site. You can take an on-line CBT course during the day as your schedule permits, access them from home by dialing into the Laboratory's network, or download them to a laptop or disk and take them with you to study at your leisure.

These materials are available to all NRL employees and contractors working on NRL projects. To access the training materials, visit our training web page at *http://amp.nrl.navy.mil/code5595/ccs-training*. You can visit the pages from any computer connected to any valid NRL network, either physically connected or dialed in through a SLIP/PPP account. For additional information, please send mail to *syssupport@nrl.navy.mil*. ■

## Keberized Fetch for Mac Users

The CCS is making available a kerberized version of fetch, the popular graphics-based file transfer utility for the Macintosh. It is posted free of charge on the CCS web-page at **http://amp.nrl.navy.mil/code5595**. Select the *Site/Volume Discount Licenses* link in the lower left hand frame, and scroll down to select *Fetch Kerberized 3.04b6sec (PPC)*. Then just fill in your name, code, and e-mail address and click the *Submit* button. ■

## VPN Dialin Services

VPN (**Virtual Private Network**) services are available for users who subscribe to non-NRL ISP accounts (DSL, cable modems or other commercial ISPs) and connect to NRL systems. Registered VPN users will be assigned a static NRL.NAVY.MIL IP address. The IP address will be downloaded to your host after authentication with the VPN server has taken place, so that your host will appear as an NRL host. The session is encrypted over the Internet from your remote system to the NRL VPN server. This establishes a virtual private network between the remote user host and local NRL systems.

The NRL VPN implementation is based on the Internet Engineering Task Force (IETF) IP-Security (IPSec) standard. We are using two Compatible Systems Intraport 2+ VPN servers (now called Cisco 5001 Concentrator) which can each support up to 500 simultaneous client-to-server tunnels or 32 site-to-site tunnels. The Intraport 2+ supports IP, IPX, AppleTalk protocols and offers a variety of client software for Windows 95/98, Windows NT, Macintosh, Linux, and Solaris. A compatible Windows 2000 client will be developed when Microsoft releases their API.

Registration for VPN and other NRL Dialin services can be found at:

*http://netgroup.nrl.navy.mil/dial-in/dial-in.html* ■

*Re: CMF.NRL.NAVY.MIL and NRL.NAVY.MIL realms*

## Note to Kerberos Users

**Background**: *Due to continual improvements in our security posture, along the ever-increasing threat, we must periodically review our policies and procedures. Occasionally, we must ask CCS users to update software, passwords, etc.*

We have recently improved our password quality verification method and to implement this, we are requiring that all CMF.NRL.NAVY.MIL and NRL.NAVY.MIL realm users change their kerberos passwords at least once every 12 months. Active users on most systems will be given a one-week warning message. Should you not use the system during this time and your password does expire, you will still have the opportunity to change it using "kpasswd" on UNIX systems or the appropriate button on PCs and Macs.

Currently, however, no password expiration times are set. To transition to this new policy without penalizing those who have changed their passwords recently, your password expiration date shall be set to 12 months from the date of your most recent password change. If it has been more than 12 months since you've changed it, your password shall be set to expire midnight on August 31, 2000.

From then on, your password will expire once per year (on the anniversary of the last change). You are, of course, allowed to change your password more frequently if you wish. ■

# Secure Shell (SSH) Install Notes

Secure Shell (SSH) is a popular software package used to provide secure encrypted remote sessions on a UNIX system over an insecure network. If you are interested in installing and configuring SSH here at the lab, these notes (with examples of a Sun/Solaris build) can be used as guidelines.

Sshd can be run from inetd although it needs to generate the server key before it can respond to the client, and this may take some time on slower systems. If you opt to use inetd to start up sshd instead of a script, remember to pass the -i flag so it behaves properly.

Linux SSH RPMs are available via ftp from *ftp.zedz.net:/pub/crypto/redhat/i386*. Wrappers support is built in and an sshd startup script is provided.

PC and Macintosh clients are available from our web site:

- windows - TeraTerm Pro 2.3
  and TSSH client

- mac - NiftyTelnet SSH

For more information about SSH, see the web page at *www.ssh.org/index.html* or check out the *comp.security.ssh* news group.

If you have problems with SSH, send email to **syssupport@nrl.navy.mil**. ■

***Visit our recently revised web pages!***

***http:/amp.nrl.navy.mil/code5595***

### 1. get ssh 1.2.27

- from our website at http://amp.nrl.navy.mil/code5595
- or from ftp.cs.hut.fi /pub/ssh
- unzip & untar

### 2. use tcp wrappers support

need the libwrap.a library from your wrappers build e.g.,

```
% setenv CC /opt/SUNWspro/bin/cc
% setenv WRAPLIBS -L/usr/sbin/libwrap.a
% ./configure --with-libwrap
```

### 3. build it

```
% make
% make install
```

### 4. create sshd entry in for tcp wrappers

- /etc/hosts.allow

```
# /etc/hosts.allow - configuration file for tcpd
sshd:132.250.0.0/255.255.0.0, \
     134.207.0.0/255.255.0.0, \
     127.0.0.0/255.255.255.0, \
     128.60.0.0/255.255.0.0
```

- /etc/hosts.deny

```
# FILE: /etc/hosts.deny
# see /etc/hosts.allow
ALL:ALL
```

### 5. mod /etc/sshd_config

```
• PermitRootLogin no
• PermitEmptyPasswords no
```

### 6. run the sshd daemon

- create startup script, e.g. /etc/rc2.d/S72sshd

```
#!/bin/sh
case “$1” in
  start)
     test -f /usr/local/sbin/sshd || exit 0
     /usr/local/sbin/sshd
     ;;
  *)
     echo “Usage: /etc/init.d/sshd { start }”
     ;;
esac
exit 0
```

- to start the sshd daemon without rebooting:

```
# /etc/rc2.d/S72sshd start
```

# Lab-wide Contracts Group

The Lab-wide Contracts Group, Code 5595, investigates, analyzes, and develops Naval Research Laboratory-wide contracts for informational systems and services. These contracts are available to the entire NRL community and offer centralized administration, cost savings, time savings (in government personnel and response to requests), convenience and flexibility. The Lab-wide hardware and software maintenance and support services contracts offer monthly and/or per-call maintenance for a large variety of computer equipment and software located within the Directorates of NRL. The table below displays the current status of the Lab-wide efforts. ■

| | ***Lab-wide Effort*** | ***Purpose*** | ***Contract Monitor*** | ***Coverage*** |
|---|---|---|---|---|
| 1. | DEC/VAX Maintenance | repair of DEC/VAX hardware and software (monthly and per call, up to 40% discount from GSA) | *Pat Kramer* | all NRL,<br>US & overseas |
| 2. | PC/Mac Hardware Maintenance | repair of PC/Mac hardware (per call, parts and labor $46.35/hr.) | *Pat Kramer* | Overlook Ave., CBD bring to Overlook, & ONR,VA |
| 3. | Generic Printer, Terminals and Tektronix Equipment | Repair of all printers, terminals, and Tektronix hardware (per call maintenance, $46.35/hr.) | *Pat Kramer* | Overlook Ave. CBD bring to Overlook, & ONR,VA |
| 4. | Generic Workstation Maintenance | repair of IBM, HP, Tektronix, NEXT, other workstations, add-ons, and software maintenance (monthly and percall, 2% discount from GSA, $77.25/hr.) | *Pat Kramer* | Overlook Ave.<br>ONR,VA<br>& Stennis, MS |
| 5. | Fore Maintenance (ATM) | maintenance for FORE systems (ATM) | *Beverly Bryant* | all NRL, remote & temp. sites |
| 6. | Silicon Graphics Maintenance | repair of SGI hardware and Software maintenance (monthly and per call, 45% discount from GSA) | *Beverly Bryant* | all NRL |
| 7. | Sun Workstation Maintenance | repair of Sun, hardware and software (monthly and per call, 38% discount from GSA) | *Beverly Bryant* | all NRL |
| 8. | Systems Support | analyst services for open systems and networking (long/short term or intermittent) | *Beverly Bryant* | Overlook Ave., Midway Research Ctr., Quantico, VA. |
| 9. | TGV Multinet Maintenance | purchase and yearly maintenance of TGV Multinet (Purchase is 25% discount, Maintenance 10%) | *Beverly Bryant* | all NRL |
| 10. | Equipment, System & Software Analysis Support Personnel | Support Personnel for Equipment and Software Analysis (Long/short term intermittent services) | *Pat Kramer* | all NRL<br>& ONR, VA |
| 11. | Networking Systems Acquisition | purchase / maintenance/services for networking / ATM equipment | *Pat Kramer* | all NRL<br>& ONR, VA. |
| 12. | Information Technology Acquisition | purchase of Information technology equipment (non-integration contract) | *Pat Kramer* | all NRL<br>& ONR, VA. |
| 13. | Software Site Licensing | purchase of software packaged products lab-wide | *Beverly Bryant* | all NRL<br>& ONR, VA. |

***Contract Monitors can be reached via phone (202) 767-1400.***